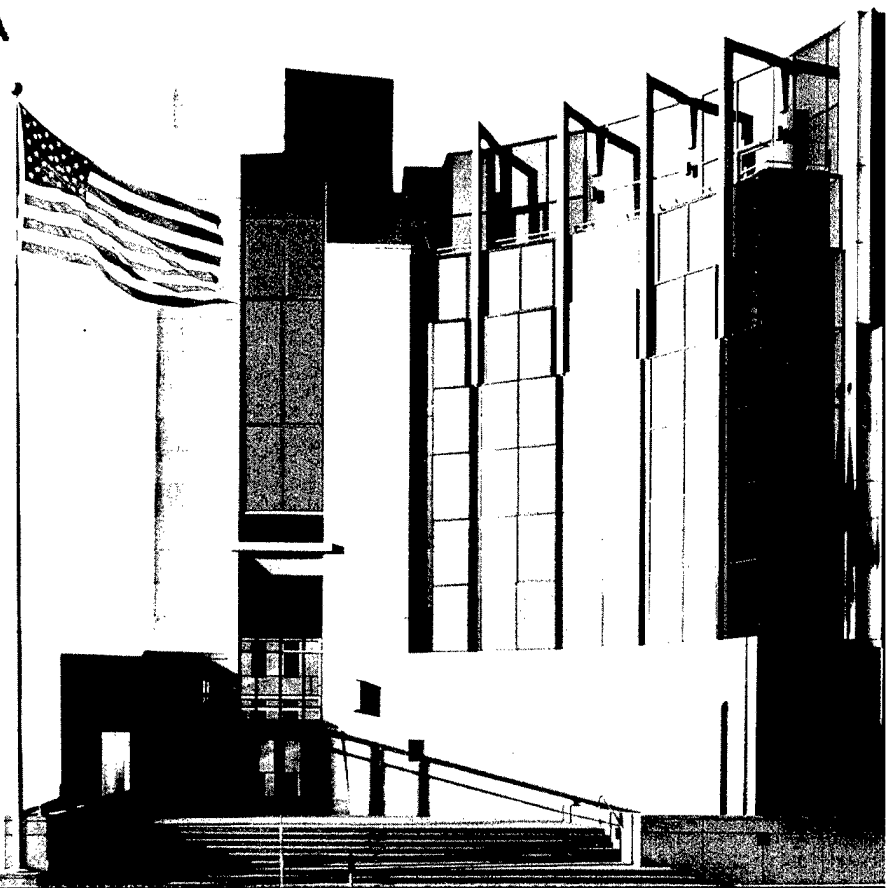
Carnegie Mellon
Software Engineering Institute

OCTAVE®-S Implementation Guide, Version 1.0

Volume 8: Critical Asset Worksheets for People

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005



HANDBOOK
CMU/SEI-2003-HB-003

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

OCTAVE®-S Implementation Guide, Version 1.0

Volume 8: Critical Asset Worksheets for People

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

Table of Contents

List of Tables

About This Document

This document is Volume 6 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides worksheets to document data related to critical assets that are categorized as people.

The volumes in this handbook are

- *Volume 1: Introduction to OCTAVE-S* – This volume provides a basic description of OCTAVE-S and advice on how to use the guide.
- *Volume 2: Preparation Guidelines* – This volume contains background and guidance for preparing to conduct an OCTAVE-S evaluation.
- *Volume 3: Method Guidelines* – This volume includes detailed guidance for each OCTAVE-S activity.
- *Volume 4: Organizational Information Workbook* – This volume provides worksheets for all organizational-level information gathered and analyzed during OCTAVE-S.
- *Volume 5: Critical Asset Workbook for Information* – This volume provides worksheets to document data related to critical assets that are categorized as information.
- *Volume 6: Critical Asset Workbook for Systems* – This volume provides worksheets to document data related to critical assets that are categorized as systems.
- *Volume 7: Critical Asset Workbook for Applications* – This volume provides worksheets to document data related to critical assets that are categorized as applications.
- ***Volume 8: Critical Asset Workbook for People*** – This volume provides worksheets to document data related to critical assets that are categorized as people.
- *Volume 9: Strategy and Plan Workbook* – This volume provides worksheets to record the current and desired protection strategy and the risk mitigation plans.
- *Volume 10: Example Scenario* – This volume includes a detailed scenario illustrating a completed set of worksheets.

Abstract

The Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

1 Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®)-S worksheets related to critical assets that are people. The activities related to these worksheets are focused on analyzing a critical asset.

Table 1 provides a brief introduction to the contents of this workbook, using activity step numbers as a key. For more details about how to complete each step, refer to the *OCTAVE®-S Method Guidelines*, which can be found in Volume 3 of the *OCTAVE®-S Implementation Guide*.

Table 1: Worksheets Provided in This Workbook

Step	Description	Worksheet	Activity	Pages
Step 6	Start a *Critical Asset Information worksheet* for each critical asset. Record the name of the critical asset on its *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information worksheet*.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 8	Record a description for each critical asset on that asset's *Critical Asset Selection worksheet*. Consider who uses each critical asset as well as who is responsible for it.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 9	Record assets that are related to each critical asset on that asset's *Critical Asset Information worksheet*. Refer to the *Asset Identification worksheet* to determine which assets are related to each critical asset.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

® OCTAVE is registered in the United States Patent and Trademark Office by Carnegie Mellon University.

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 26	Transfer the stoplight status for each security practice area from the *Security Practices worksheet* to the "Security Practice Areas" section (Step 26) of each critical asset's *Risk Profile worksheet.*	Risk Profile Security Practices	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-24
Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.	Risk Profile	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-24

2 Critical Asset Information Worksheet for People

Phase 1
Process S2
Activity S2.1

Step 6	Start a *Critical Asset Information worksheet* for each critical asset. Record the name of the critical asset on its *Critical Asset Information worksheet.*
Step 7	Record your rationale for selecting each critical asset on that asset's *Critical Asset Information worksheet.*
Step 8	Record a description for each critical asset on that asset's *Critical Asset Selection worksheet.* Consider who uses each critical asset as well as who is responsible for it.
Step 9	Record assets that are related to each critical asset on that asset's *Critical Asset Information worksheet.* Refer to the *Asset Identification worksheet* to determine which assets are related to each critical asset.

Phase 1
Process S2
Activity S2.2

Step 10	Record the security requirements for each critical asset on that asset's *Critical Asset Information worksheet.*
Step 11	For each critical asset, record the most important security requirement on that asset's *Critical Asset Information worksheet.*

Step 8

Description
What special skills or knowledge are provided by this person(s)?

Step 10

Security Requirements		**Step 11** **Most Important Security Requirement**
What are the security requirements for this person(s)? *(Hint: Focus on what the security requirements should be, not what they currently are.)*		*Which security requirement is most important for this person(s)?*
❑ Availability	The set of skills provided by_____ must be available when needed.	❑ Availability ❑ Other
❑ Other	_____ _____	

3 Risk Profile Worksheet for People – Other Problems

Phase 1
Process S2
Activity S2.3

Step 12	Complete the threat tree for *other problems*. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the *Threat Translation Guide* (see pp. 26-30 of this workbook).
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.

continued

Basic Risk Profile | **Other Problems**

Step 24 | **Step 26** | **Step 27**

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value **Confidence**

Very | Somewhat | Not At All

Security Practice Areas

What is the stoplight status for each security practice area?

Strategic

1. Sec Training
2. Sec Strategy
3. Sec Mgmt
4. Sec Policy & Reg
5. Coll Sec Mgmt
6. Cont Planning

Operational

7. Phys Acc Cntrl
8. Monitor Phys Sec
9. Sys & Net Mgmt
10. Monitor IT Sec
11. Authen & Auth
12. Vul Mgmt
13. Encryption
14. Sec Arch & Des
15. Incident Mgmt

Approach

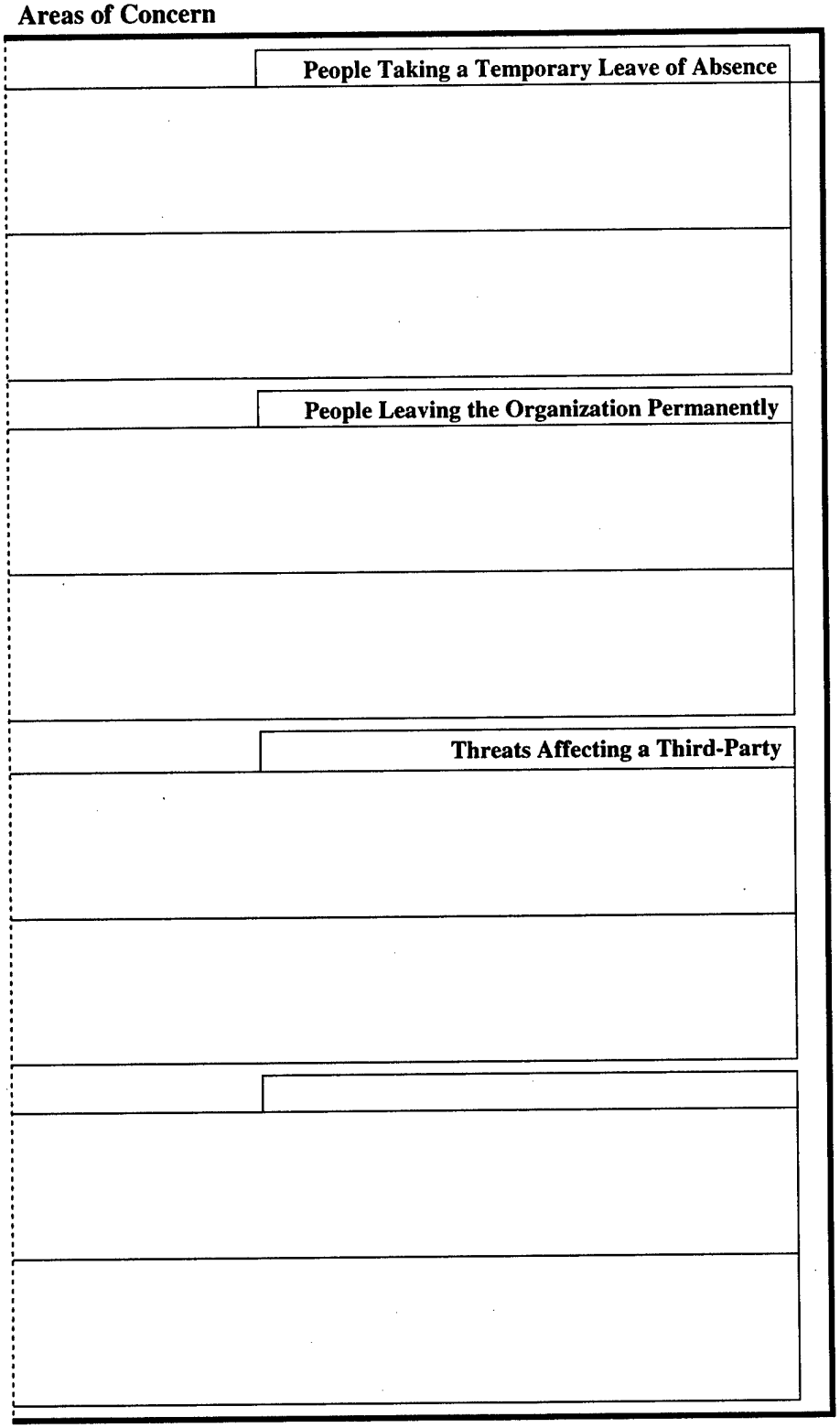
What is your approach for addressing each risk?

Accept | Defer | Mitigate

Threat Context | **Other Problems**

Notes
What additional notes about each threat do you want to record?

Areas of Concern



Basic Risk Profile

Other Problems (cont.)

Step 24

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value **Confidence**

Very | Somewhat | Not At All

Step 26

Security Practice Areas

What is the stoplight status for each security practice area?

Strategic

1. Sec Training
2. Sec Strategy
3. Sec Mgmt
4. Sec Policy & Reg
5. Coll Sec Mgmt
6. Cont Planning

Operational

7. Phys Acc Cntrl
8. Monitor Phys Sec
9. Sys & Net Mgmt
10. Monitor IT Sec
11. Authen & Auth
12. Vul Mgmt
13. Encryption
14. Sec Arch & Des
15. Incident Mgmt

Step 27

Approach

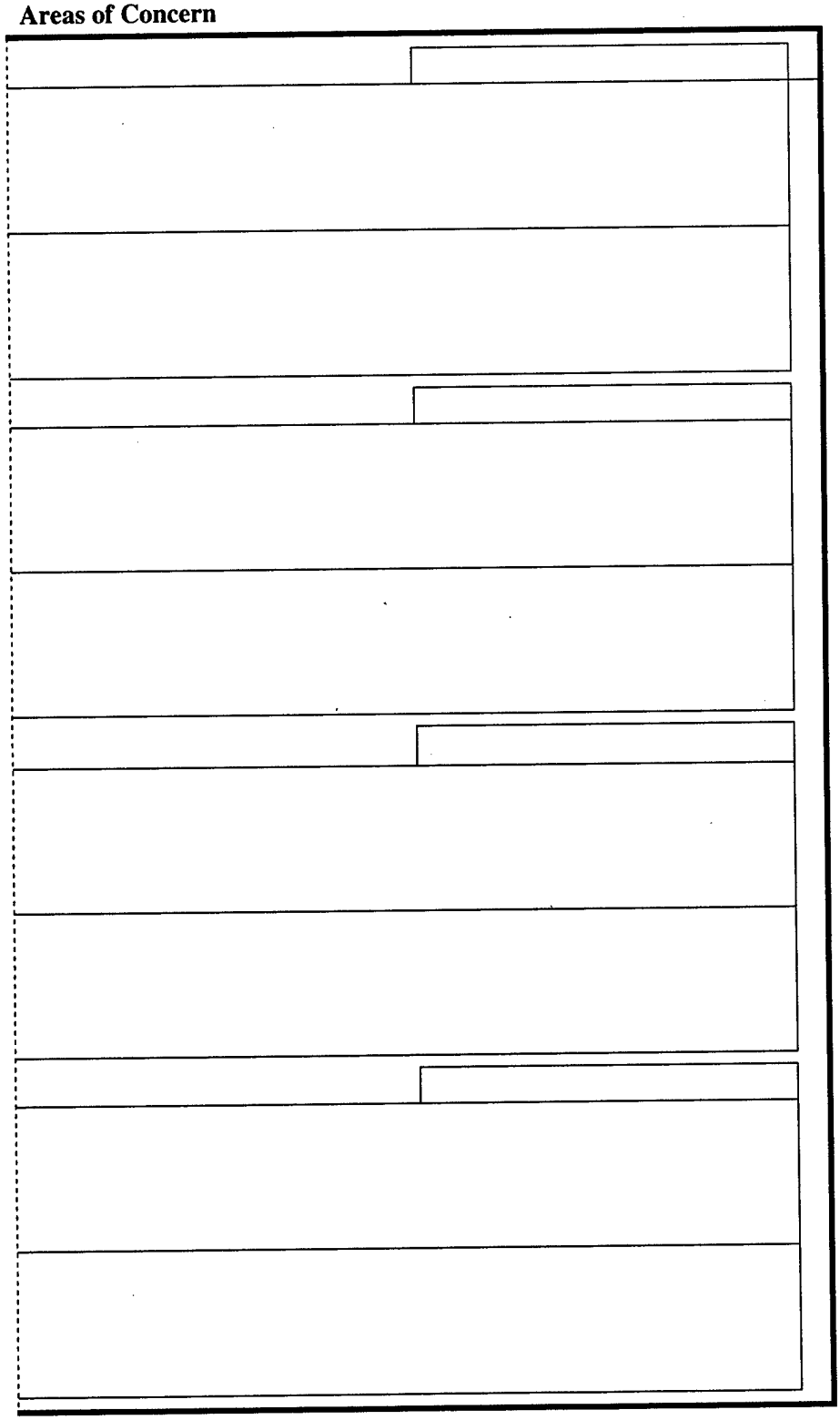
What is your approach for addressing each risk?

Accept | Defer | Mitigate

Threat Context | **Other Problems (cont.)**

Notes
What additional notes about each threat do you want to record?

Areas of Concern



4 Threat Translation Guide

Phase 1
Process S2
Activity S2.3

Threat Translation Guide

The *Threat Translation Guide* describes each branch of an asset-based threat tree. If you have difficulty understanding the types of threats represented by a branch, you can use this guide to decipher the meaning of that branch.

You will find asset-based threat trees for the following sources of threat:

Source of Threat	Page
Other problems	26-30

Description	Example*
---	---
---	---
---	---
A staff member(s) with unique knowledge or a unique skill takes a temporary leave of absence from an organization. The organization does not have any other staff members with comparable skills, resulting in an interruption of access to the unique knowledge or skill.	A key member of the IT group in a small organization takes a leave of absence to care for an ill family member. This member of the IT staff is responsible for maintaining a legacy order entry system. No other staff members know how to maintain the system. The organization has a temporary interruption of access to a vital skill that is important to its business operations.
---	---
---	---
---	---
A staff member(s) with unique knowledge or a unique skill leaves an organization permanently. The organization does not have any other staff members with comparable skills, resulting in an interruption of access to the unique knowledge or skill until a replacement if hired.	A clerk is responsible for entering data into a database system. The clerk, who is currently the only one at the company who understands how to use the system, unexpectedly leaves for a better position at another company. The organization no longer has access to a skill that is important to its business operations until a replacement is hired and trained.

Description	Example*
---	---
---	---
---	---
An organization depends on a third party for a particular service. Any threats to the third party that prevents them from fulfilling their obligations results in an interruption of service to the organization.	A service provider maintains the computing infrastructure for a manufacturing company. A shop floor scheduling system is physically located at the service provider's site. A disgruntled staff member employed by the service provider plants a software "time bomb" that takes down the service provider's networks for several days. The manufacturing site's access to the shop floor scheduling system is interrupted until the service provider can get its infrastructure running again.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	January 2005	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE-S Implementation Guide, Version 1.0, Volume 8	F19628-00-C-0003

6. AUTHOR(S)

Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2003-HB-003

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

The Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk management, OCTAVE	30

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL